	L #	Search Text	DBs	Time Stamp	Hits
1	L1	mertes.in. and paul.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:55	20
2	L2	mettken.in. and werner.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:56	6
3	L3	L1 and L2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:56	1

	L #	Search Text	DBs	Time Stamp	Hits
4	L4	deutsche.asn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:56	9568
5	L5	L3 and L4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:56	1
6	L6	713/156.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:56	950

	L #	Search Text	DBs	Time Stamp	Hits
7	L7	713/156.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:57	19
8	L8	713/158.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:57	2
9	L9	380/277.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:57	23

	L #	Search Text	DBs	Time Stamp	Hits
10	L10	380/278.ccls. and (generating) and (asymmetrical) and (cryptographic keys)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:58	19
11	L11	"generat$3" near "asymmetrical cryptokey" near "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:59	0
12	L12	"generat$3" same "asymmetrical cryptokey" near "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 11:59	0

	L #	Search Text	DBs	Time Stamp	Hits
13	L13	"generat$3" same "asymmetrical cryptokey" same "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:00	0
14	L14	(generat$3) same "asymmetrical cryptokey" same "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:00	0
15	L15	(generat$3) and "asymmetrical cryptokey" and "user"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:00	0

	L #	Search Text	DBs	Time Stamp	Hits
16	L16	"asymmetrical cryptokey" and "user" and "trust center"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:00	0
17	L17	"trust center" and "user" and "certified signature" and "key pair"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:01	1
18	L18	"encryption key pair" and "public" and "secret"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:01	235

	L #	Search Text	DBs	Time Stamp	Hits
19	L19	(encrypt$3) same (certificate) same (encryption key pair)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:01	9008
20	L20	L18 and L19	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:01	131
21	L21	L20 and "bilateral communication"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:02	0

	L #	Search Text	DBs	Time Stamp	Hits
22	L22	L20 and "no communication"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:02	3
23	L23	L22 and "genuineness" and "validity"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	2007/12/07 12:02	0

Interference Search

	Type	L #	Search Text	DBs	Time Stamp	Hits
24	BRS	L24	generating AND certifying AND asymmetrical AND cryptokey AND trust AND center AND user AND secure AND transmission.CLM.	US-PGPUB	2007/12/07 12:03	0
25	BRS	L25	trust AND center AND user AND encryption AND key AND pair AND certified AND signature.CLM.	US-PGPUB	2007/12/07 12:03	59
26	BRS	L26	part AND secret AND public AND encryption AND key AND pair AND certified AND signature.CLM.	US-PGPUB	2007/12/07 12:04	259
27	BRS	L27	marking AND public AND part AND encryption AND key AND pair AND trust AND center.CLM.	US-PGPUB	2007/12/07 12:04	58
28	BRS	L28	unequivocally AND assigning AND one AND encryption AND key AND pair.CLM.	US-PGPUB	2007/12/07 12:04	0
29	BRS	L29	new AND certificate AND encrypted AND user.CLM.	US-PGPUB	2007/12/07 12:04	4062
30	BRS	L30	checking AND correctness AND bilateral AND communication AND verifying AND signature.CLM.	US-PGPUB	2007/12/07 12:04	1
31	BRS	L31	checking AND genuineness AND validity AND new AND certificate AND trust AND center.CLM.	US-PGPUB	2007/12/07 12:04	1

Web Images Maps News Products Gmail more ▾ Sign in

Google asymmetrical, trust center, certificate, digital si Search Advanced Search Preferences

Web Results **1 - 10** of about **36** for **asymmetrical, trust center, certificate, digital signature, unequivocal "cr**

Did you mean: asymmetrical, ***thrust*** center, certificate, digital signature, unequivocal "cryptographic keys"

Emerald FullText Article : Certificates and **trust** in electronic ...
Public key - also know as **asymmetric** - cryptography uses different keys for A **digital certificate** provides any recipient of a **digital signature** with a ...
xtra.emeraldinsight.com/.../viewContentItem.do?contentType=Article&hdAction=lnkhtml&contentId=862702 - Similar pages

Certificates and **trust** in electronic commerce Certificates and ...
certificate; if you **trust** the CA, then you can. **trust** the signer's identity. What is more, the. **digital signature** of the CA on the **certificate** ...
www.emeraldinsight.com/Insight/html/Output/Published/EmeraldFullTextArticle/Pdf/0460050504.pdf - Similar pages

[PDF] Privacy and Security Threat Analysis of the Federal Employee ...
File Format: PDF/Adobe Acrobat - View as HTML
an **asymmetric** key pair and corresponding **certificate**, and two bio-. metric fingerprints.
The German DIN standards [8, 9] for **digital signature** cards ...
cups.cs.cmu.edu/soups/2006/proceedings/p114_karger.pdf - Similar pages

[PDF] THE ROLES OF AUTHENTICATION, AUTHORIZATION & CRYPTOGRAPHY IN ...
File Format: PDF/Adobe Acrobat - View as HTML
FIPS 201 **Cryptographic Keys**, **Digital**. Certificates and **Digital Signatures**. FIPS 201 specifies that, at a minimum, the PIV. Card must store one **asymmetric** ...
www.corestreet.com/about/library/datasheets/QTU_Q405.pdf - Similar pages

[DOC] The Use of Public Key Technology in Securing Critical Infrastructures
File Format: Microsoft Word - View as HTML
Access with **Trust** described agency pilot efforts using public key To obtain a **digital signature certificate**, RDA and FSA users are required to appear ...
www.cio.gov/fpkisc/library/pkireport053100.doc - Similar pages

[DOC] The Use of Public Key Technology in Securing Critical Infrastructures
File Format: Microsoft Word - View as HTML
Each client created a **certificate trust** path between the domain of the recipient and To obtain a **digital signature certificate**, RDA and FSA users are ...
cio.nist.gov/esd/emaildir/lists/pki-twg/doc00009.doc - Similar pages

[PDF] E ditorial I mpressum
File Format: PDF/Adobe Acrobat - View as HTML
duces a public key **certificate** by applying this. same **digital signature** process to the sender's tains **asymmetric** S-Boxes" bit will be set in the sta- ...
www.silicon-**trust**.com/html-data/pdf/secure_3/Secure3_kmpl.pdf - Similar pages

Digital Commons: Browse by Title
One well-known method of providing authentication in GKA protocols is through the use of **digital signatures**. Traditional **certificate**-based **signature** schemes ...
digitalcom.thei3p.org/browse_by_title.html?title=e* - 305k - Cached - Similar pages

[PDF] eTendering – Security and Legal Issues
File Format: PDF/Adobe Acrobat - View as HTML
CA vouches for the validity of the public key by digitally signing the **certificate**. All users in the. community must **trust** the **digital signature** of the CA. ...
www.construction-innovation.info/index.php?id=912 - Similar pages

[DOC] MKE
File Format: Microsoft Word - View as HTML
In concrete, a common **digital signature** and **certificate** validation TC **Trustcenter** and Telesec will provide certificates and **signatures** on the basis ...
www.cni.cz/NP/NotesPortalCNI.nsf/key/1F6F6E30CA06B750C1256FAF005072F9/$File/Final%20Draft.doc - Similar pages

Did you mean to search for: asymmetrical, ***thrust*** center, certificate, digital signature, unequivocal "cryptographic keys"

1 2 3 4 **Next**

Try Google Desktop: search your computer as easily as you search the web.

asymmetrical, trust center, certificate Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

©2007 Google - Google Home - Advertising Programs - Business Solutions - About Google

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

+cryptographic +keys, +signature, +certificate, +trust, +key SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used:
cryptographic keys signature certificate trust key pair unequivocal

Found **353** of **215,737**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Extending cryptographic logics of belief to key agreement protocols

Paul van Oorschot

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**

Publisher: ACM Press

Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references, citings, index terms

The authentication logic of Burrows, Abadi and Needham (BAN) provided an important step towards rigourous analysis of authentication protocols, and has motivated several subsequent refinements. We propose extensions to BAN-like logics which facilitate, for the first time, examination of public-key based authenticated key establishment protocols in which both parties contribute to the derived key (i.e. key agreement protocols). Attention is focussed on six distinct generic goals for authenti ...

2 Risk transparency: Privacy and security threat analysis of the federal employee personal identity verification (PIV) program

Paul A. Karger

July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**

Publisher: ACM Press

Full text available: pdf(113.11 KB) Additional Information: full citation, abstract, references, index terms

This paper is a security and privacy threat analysis of new Federal Information Processing Standard for Personal Identity Verification (FIPS PUB 201). It identifies some problems with the standard, and it proposes solutions to those problems, using standardized cryptographic techniques that are based on the Internet Key Exchange (IKE) protocol [16]. When the standard is viewed in the abstract, it seems to effectively provide security and privacy, because it uses strong cryptographic algorithms. ...

Keywords: personal identification, privacy, smart cards

3 A survey on peer-to-peer key management for mobile ad hoc networks

Johann Van Der Merwe, Dawoud Dawoud, Stephen McDonald

April 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 1

Publisher: ACM Press

Full text available: pdf(872.71 KB) Additional Information: full citation, abstract, references, index terms

The article reviews the most popular peer-to-peer key management protocols for mobile ad hoc networks (MANETs). The protocols are subdivided into groups based on their design strategy or main characteristic. The article discusses and provides comments on the strategy of each group separately. The discussions give insight into open research problems in the area of pairwise key management.

Keywords: Mobile ad hoc networks, pairwise key management, peer-to-peer key management, security

4 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

5 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure

Albert Levi, M. Ufuk Caglayan, Cetin K. Koc

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

6 Equipping smart devices with public key signatures

Xuhua Ding, Daniele Mazzocchi, Gene Tsudik

February 2007 **ACM Transactions on Internet Technology (TOIT)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(274.64 KB) Additional Information: full citation, abstract, references, index terms

One of the major recent trends in computing has been towards so-called smart devices, such as PDAs, cell phones and sensors. Such devices tend to have a feature in common: limited computational capabilities and equally limited power, as most operate on batteries. This makes them ill-suited for public key signatures. This article explores practical and conceptual implications of using Server-Aided Signatures (SAS) for these devices. SAS is a signature method that relies on partially-trusted serve ...

Keywords: Digital signatures, public key infrastructure

7 COCA: A secure distributed online certification authority

Lidong Zhou, Fred B. Schneider, Robbert Van Renesse
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(448.28 KB) Additional Information: full citation, abstract, references, citings, index terms

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no assumption is made about execution speed and message delivery delays; channels are expected to exhibit only intermittent reliability; and with $3t + 1$ COCA servers up to t may be faulty or compromised. COCA is the first system to integr ...

Keywords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

8 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent
October 1999 **Wireless Networks**, Volume 5 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

9 Cryptosystems & analysis: Self-Generated-Certificate Public Key Cryptography and certificateless signature/encryption scheme in the standard model: extended abstract

Joseph K. Liu, Man Ho Au, Willy Susilo
March 2007 **Proceedings of the 2nd ACM symposium on Information, computer and communications security ASIACCS '07**
Publisher: ACM Press
Full text available: pdf(444.72 KB) Additional Information: full citation, abstract, references

Certificateless Public Key Cryptography (CL-PKC) enjoys a number of features of Identity-Based Cryptography (IBC) while without having the problem of key escrow. However, it *does* suffer from an attack where the adversary, Carol, replaces Alice's public key by someone's public key so that Bob, who wants to send an encrypted message to Alice, uses Alice's identity and other's public key as the inputs to the encryption function. As a result, Alice cannot decrypt the message while Bob is u ...

Keywords: certificateless encryption, certificateless signature

10 (How) can mobile agents do secure electronic transactions on untrusted hosts? A

survey of the security issues and the current solutions
Joris Claessens, Bart Preneel, Joos Vandewalle
February 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 1
Publisher: ACM Press

Full text available: pdf(197.96 KB) Additional Information: full citation, abstract, references, citings, index terms

This article investigates if and how mobile agents can execute secure electronic transactions on untrusted hosts. An overview of the security issues of mobile agents is first given. The problem of untrusted (i.e., potentially malicious) hosts is one of these issues, and appears to be the most difficult to solve. The current approaches to counter this problem are evaluated, and their relevance for secure electronic transactions is discussed. In particular, a state-of-the-art survey of mobile agen ...

Keywords: Mobile agent security, electronic transactions, malicious hosts

11 General storage protection techniques: Securing distributed storage: challenges, techniques, and systems
Vishal Kher, Yongdae Kim
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(294.61 KB) Additional Information: full citation, abstract, references, index terms

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention and protection have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related to storage and present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of the storage security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

12 Identification control: Public key distribution through "cryptoIDs"
Trevor Perrin
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press
Full text available: pdf(1.51 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we argue that person-to-person key distribution is best accomplished with a key-centric approach, instead of PKI: users should distribute public key fingerprints in the same way they distribute phone numbers, postal addresses, and the like. To make this work, fingerprints need to be *small*, so users can handle them easily; *multipurpose*, so only a single fingerprint is needed for each user; and *long-lived*, so fingerprints don't have to be frequently redistribute ...

Keywords: cryptoIDs, fingerprints, key distribution, key management, public key infrastructure

13 Privacy through pseudonymity in user-adaptive systems
Alfred Kobsa, Jörg Schreck
May 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 2

Publisher: ACM Press

Full text available: pdf(881.69 KB) Additional Information: full citation, abstract, references, citings, index terms, review

User-adaptive applications cater to the needs of each individual computer user, taking for example users' interests, level of expertise, preferences, perceptual and motoric abilities, and the usage environment into account. Central user modeling servers collect and process the information about users that different user-adaptive systems require to personalize their user interaction.Adaptive systems are generally better able to cater to users the more data their user modeling systems collect and ...

Keywords: Chaum mix, KQML, User modeling, access control, anonymity, encryption, personal information, personalization, privacy, pseudonymity, reference model, secrecy, security, user-adaptive systems

14 Credentials: Direct anonymous attestation

Ernie Brickell, Jan Camenisch, Liqun Chen

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

Publisher: ACM Press

Full text available: pdf(314.67 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes the direct anonymous attestation scheme (DAA). This scheme was adopted by the Trusted Computing Group (TCG) as the method for remote authentication of a hardware module, called Trusted Platform Module (TPM), while preserving the privacy of the user of the platform that contains the module. DAA can be seen as a group signature without the feature that a signature can be opened, i.e., the anonymity is not revocable. Moreover, DAA allows for pseudonyms, i.e., for each signat ...

Keywords: anonymous credential systems, cryptographic protocols, integrity based computing, privacy, trusted computing

15 Fine-grained control of security capabilities

Dan Boneh, Xuhua Ding, Gene Tsudik

February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1

Publisher: ACM Press

Full text available: pdf(128.09 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocat ...

Keywords: Certificate Revocation, Digital Signatures, Public Key Infrastructure

16 Secure sessions for Web services

Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, Andrew D. Gordon

May 2007 **ACM Transactions on Information and System Security (TISSEC)**, Volume 10 Issue 2

Publisher: ACM Press

Full text available: Additional Information:

pdf(579.98 KB) full citation, abstract, references, index terms

We address the problem of securing sequences of SOAP messages exchanged between web services and their clients. The WS-Security standard defines basic mechanisms to secure SOAP traffic, one message at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; moreover, it is often important to secure the integrity of a whole session, as well as each message. To these ends, recent specifications provide further SOAP-level mechanisms. WS-S ...

Keywords: Web services, XML security

17 Authentication and signature schemes: On the performance, feasibility, and use of forward-secure signatures

Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**

Publisher: ACM Press

Full text available: pdf(386.51 KB) Additional Information: full citation, abstract, references, citings, index terms

Forward-secure signatures (FSSs) have recently received much attention from the cryptographic theory community as a potentially realistic way to mitigate many of the difficulties digital signatures face with key exposure. However, no previous works have explored the practical performance of these proposed constructions in real-world applications, nor have they compared FSS to traditional, non-forward-secure, signatures in a non-asymptotic way.We present an empirical evaluation of several FSS sch ...

Keywords: digital signatures, forward-secure signatures

18 Encryption and Secure Computer Networks

Gerald J. Popek, Charles S. Kline

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4

Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

19 SPV: secure path vector routing for securing BGP

Yih-Chun Hu, Adrian Perrig, Marvin Sirbu

August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, citings, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

20 A secure authentication and billing architecture for wireless mesh networks

Yanchao Zhang, Yuguang Fang
October 2007 **Wireless Networks**, Volume 13 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(501.79 KB) Additional Information: full citation, abstract, references, index terms

Wireless mesh networks (WMNs) are gaining growing interest as a promising technology for ubiquitous high-speed network access. While much effort has been made to address issues at physical, data link, and network layers, little attention has been paid to the security aspect central to the realistic deployment of WMNs. We propose UPASS, the first known secure authentication and billing architecture for large-scale WMNs. UPASS features a novel user-broker-operator trust model built upon the con ...

Keywords: authentication, billing, roaming, security, wireless mesh networks (WMNs)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

IEEE Xplore® RELEASE 2.4

Home | Login | Logout | Access Information | Alerts | Purchase History |

Welcome United States Patent and Trademark Office

□ Search Results BROWSE SEARCH IEEE XPLORE GUIDE

Results for "(((encryption keys)<in>metadata) <and> ((encryption)<in>metadata))"
Your search matched **117** of **1700278** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

New [Beta] Application Notes POWERED BY GLOBALSPEC

Modify Search

(((encryption keys)<in>metadata) <and> ((encryption)<in>metadata)) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Search Options

View Session History

New Search

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

IEEE/IET Books Educational Courses A

IEEE/IET journals, transactions, letters, magazines, conference proceedings, and

view selected items Select All Deselect All View: 1

1. **Enhanced protocols for hierarchical encryption key management for sec internet environments**
Lu, W.P.; Sundareshan, M.K.;
Communications, IEEE Transactions on
Volume 40, Issue 4, April 1992 Page(s):658 - 660
Digital Object Identifier 10.1109/26.141416
AbstractPlus | Full Text: PDF(244 KB) IEEE JNL
Rights and Permissions

2. **Feasibility of generating biometric encryption keys**
Hoque, S.; Fairhurst, M.; Howells, G.; Deravi, F.;
Electronics Letters
Volume 41, Issue 6, 17 March 2005 Page(s):309 - 311
Digital Object Identifier 10.1049/el:20057524
AbstractPlus | Full Text: PDF(437 KB) IET JNL

3. **Multi-user quantum cryptography networks**
Wang, B.C.;
Wireless and Optical Communications, 2005. 14th Annual WOCC 2005. Inter
22-23 April 2005 Page(s):78
Digital Object Identifier 10.1109/WOCC.2005.1553760
AbstractPlus | Full Text: PDF(151 KB) IEEE CNF
Rights and Permissions

4. **A centralized key management scheme for hierarchical access control**
Zhang, Q.; Wang, Y.;
Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE
Volume 4, 29 Nov.-3 Dec. 2004 Page(s):2067 - 2071 Vol.4
Digital Object Identifier 10.1109/GLOCOM.2004.1378375
AbstractPlus | Full Text: PDF(575 KB) IEEE CNF
Rights and Permissions

5. **A key assignment scheme for controlling access in partially ordered use**
Chin-Chen Chang; Iuon-Chang Lin; Hui-Min Tsai; Hsiao-Hsi Wang;

Advanced Information Networking and Applications, 2004. AINA 2004. 18th Ir
Volume 2, 2004 Page(s):376 - 379 Vol.2
Digital Object Identifier 10.1109/AINA.2004.1283826

AbstractPlus | Full Text: PDF(320 KB) IEEE CNF
Rights and Permissions

6. **Complexity measure of encryption keys used for securing computer net**
Bahie-Eldin, M.A.; Omar, A.A.;
Computer Security Applications Conference, 1998, Proceedings., 14th Annua
7-11 Dec. 1998 Page(s):250 - 255
Digital Object Identifier 10.1109/CSAC.1998.738645

AbstractPlus | Full Text: PDF(864 KB) IEEE CNF
Rights and Permissions

7. **Message encryption in a X.400 message handling system**
Tse, K.W.; Chow, K.P.;
TENCON 90. 1990 IEEE Region 10 Conference on Computer and Communic
24-27 Sept. 1990 Page(s):432 - 436 vol.1
Digital Object Identifier 10.1109/TENCON.1990.152648

AbstractPlus | Full Text: PDF(260 KB) IEEE CNF
Rights and Permissions

8. **Key Generation for Secure Inter-satellite Communication**
Papoutsis, Evangelos; Howells, Gareth; Hopkins, Andrew; McDonald-Maier, K
Adaptive Hardware and Systems, 2007. AHS 2007. Second NASA/ESA Conf
5-8 Aug. 2007 Page(s):671 - 681
Digital Object Identifier 10.1109/AHS.2007.67

AbstractPlus | Full Text: PDF(269 KB) IEEE CNF
Rights and Permissions

9. **On the impact of GSM encryption and man-in-the-middle attacks on the : GSM/UMTS networks**
Meyer, U.; Wetzel, S.;
Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15t
Symposium on
Volume 4, 5-8 Sept. 2004 Page(s):2876 - 2883 Vol.4

AbstractPlus | Full Text: PDF(1119 KB) IEEE CNF
Rights and Permissions

10. **On the shannon cipher system with a capacity-limited key-distribution c**
Merhav, N.;
Information Theory, IEEE Transactions on
Volume 52, Issue 3, March 2006 Page(s):1269 - 1273
Digital Object Identifier 10.1109/TIT.2005.864448

AbstractPlus | Full Text: PDF(204 KB) IEEE JNL
Rights and Permissions

11. **Key Management Standards Hit the Fast Track**
Goth, Greg;
Distributed Systems Online, IEEE
Volume 8, Issue 9, Sept. 2007 Page(s):4 - 4
Digital Object Identifier 10.1109/MDSO.2007.4370100

AbstractPlus | Full Text: PDF(157 KB) IEEE JNL
Rights and Permissions

12. **Java card: Internet computing on a smart card**
Guthery, S.B.;
Internet Computing, IEEE
Volume 1, Issue 1, Jan.-Feb. 1997 Page(s):57 - 59

Digital Object Identifier 10.1109/4236.585173

AbstractPlus | Full Text: PDF(100 KB) IEEE JNL
Rights and Permissions

13. **Privacy and authentication protocols for PCS**
Mohan, S.;
Personal Communications, IEEE [see also IEEE Wireless Communications]
Volume 3, Issue 5, Oct. 1996 Page(s):34 - 38
Digital Object Identifier 10.1109/98.542236

AbstractPlus | Full Text: PDF(1652 KB) IEEE JNL
Rights and Permissions

14. **Perceptual cryptography on MPEG Layer III bit-streams**
Torrubia, A.; Mora, F.;
Consumer Electronics, IEEE Transactions on
Volume 48, Issue 4, Nov 2002 Page(s):1046 - 1050
Digital Object Identifier 10.1109/TCE.2003.1196437

AbstractPlus | Full Text: PDF(345 KB) IEEE JNL
Rights and Permissions

15. **Distributed servers approach for large-scale secure multicast**
Kin-Ching Chan; Chan, S.-H.G.;
Selected Areas in Communications, IEEE Journal on
Volume 20, Issue 8, Oct. 2002 Page(s):1500 - 1510
Digital Object Identifier 10.1109/JSAC.2002.803966

AbstractPlus | References | Full Text: PDF(383 KB) IEEE JNL
Rights and Permissions

16. **Cryptanalysis of frequency domain analogue speech scramblers**
Goldburg, B.; Sridharan, S.; Dawson, E.;
Communications, Speech and Vision, IEE Proceedings I
Volume 140, Issue 4, Aug. 1993 Page(s):235 - 239

AbstractPlus | Full Text: PDF(356 KB) IET JNL

17. **Considerations of Extending SQL on Encrypted Data in UniSQL**
Yong Soon Kim; Eui Kyeong Hong;
Advanced Communication Technology, The 9th International Conference on
Volume 1, 12-14 Feb. 2007 Page(s):587 - 590
Digital Object Identifier 10.1109/ICACT.2007.358424

AbstractPlus | Full Text: PDF(5112 KB) IEEE CNF
Rights and Permissions

18. **Image Encryption and Decryption Using SCAN Methodology**
Chao-Shen Chen; Rong-Jian Chen;
Parallel and Distributed Computing, Applications and Technologies, 2006. PD
International Conference on
Dec. 2006 Page(s):61 - 66
Digital Object Identifier 10.1109/PDCAT.2006.71

AbstractPlus | Full Text: PDF(449 KB) IEEE CNF
Rights and Permissions

19. **An RSSI-based scheme for sybil attack detection in wireless sensor net**
Demirbas, M.; Youngwhan Song;
World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. I
a
26-29 June 2006 Page(s):5 pp.
Digital Object Identifier 10.1109/WOWMOM.2006.27

AbstractPlus | Full Text: PDF(248 KB) IEEE CNF
Rights and Permissions

20. **Secure group communication based scheme for differential access cont environments**
Karandikar, Y.; Zou, X.; Dai, Y.;
Parallel and Distributed Systems, 2005. Proceedings. 11th International Conf
Volume 2, 20-22 July 2005 Page(s):448 - 452 Vol. 2
Digital Object Identifier 10.1109/ICPADS.2005.260
AbstractPlus | Full Text: PDF(240 KB) IEEE CNF
Rights and Permissions

21. **A note on broadcast encryption key management with applications to la systems**
Guoqiang Shu; Lee, D.; Yannakakis, M.;
Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th Inte
25-29 April 2006 Page(s):8 pp.
Digital Object Identifier 10.1109/IPDPS.2006.1639680
AbstractPlus | Full Text: PDF(192 KB) IEEE CNF
Rights and Permissions

22. **A new way of generating grid-scroll chaos and its application to biometr**
Han, F.; Yu, X.; Hu, J.;
Industrial Electronics Society, 2005. IECON 2005. 32nd Annual Conference o
6-10 Nov. 2005 Page(s):6 pp.
Digital Object Identifier 10.1109/IECON.2005.1568879
AbstractPlus | Full Text: PDF(594 KB) IEEE CNF
Rights and Permissions

23. **Cryptographic data security in wireless networks based on biometrical p**
Vishnyakov, D.V.; Serdyukov, A.G.;
Control and Communications, 2005. SIBCON '05. IEEE International Siberian
21-22 Oct. 2005 Page(s):52 - 54
Digital Object Identifier 10.1109/SIBCON.2005.1611191
AbstractPlus | Full Text: PDF(216 KB) IEEE CNF
Rights and Permissions

24. **Voice over IP security and law enforcement**
Thanthry, N.; Pendse, R.; Namuduri, K.;
Security Technology, 2005. CCST '05. 39th Annual 2005 International Carnal
11-14 Oct. 2005 Page(s):246 - 250
Digital Object Identifier 10.1109/CCST.2005.1594888
AbstractPlus | Full Text: PDF(472 KB) IEEE CNF
Rights and Permissions

25. **A new image encryption algorithm based on inversable functions define**
Seripearlu, L.; Frunza, M.D.;
Signals, Circuits and Systems, 2005. ISSCS 2005. International Symposium o
Volume 1, 14-15 July 2005 Page(s):243 - 246 Vol. 1
Digital Object Identifier 10.1109/ISSCS.2005.1509899
AbstractPlus | Full Text: PDF(227 KB) IEEE CNF
Rights and Permissions

View: 1

Indexed by Inspec®
© Copyright 20